UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The entire property located at 2611 S. Shore Drive, Milwaukee, Wisconsin, including the residential building, any outbuildings, and any appurtenances thereto. 2611 S. Shore Drive, Milwaukee, Wisconsin, more fully described in Attachment A.

Case No. 20-1068M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Section 2252(a)(2)	Distribution of Child Pornography

The application is based on these facts:

See affached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

George Mason
Applicant's signature

FBI SA George Mason
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: October 26, 2020

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, George Kyle Mason, being first duly sworn, hereby depose and state as follows:

1. I am employed as a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since 2017. I am currently assigned to the FBI Milwaukee Division, Child Exploitation Task Force. My duties include investigating criminal violations relating to child sexual exploitation and child pornography. I have experience investigating criminal violations related to both State and Federal laws, including executing search warrants and conducting interviews of individuals involved in trading child pornography. I have also received training in investigating and enforcing State and Federal child pornography laws in which computers and other digital media are used as a means for receiving, transmitting, and storing child pornography. Prior to becoming a Special Agent, I was a sworn Kansas Law Enforcement Police Officer in the City of Prairie Village, Kansas. I participated in various criminal investigations as a Detective including, but not limited to, sexual exploitation of a child, coercion and enticement of a minor to engage in sexual conduct, and sexual abuse of a minor.

2. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law enforcement officers, who have provided information to me during the course of their official duties and whom I consider truthful and reliable. Some of the information was provided in response to administrative subpoenas and I believe this information to be also be reliable.

3. Based upon the information described below, I submit that probable cause exists to believe that someone residing at 2611 South Shore Drive, Milwaukee, Wisconsin (the Subject Premises) has committed the crime of distributing child pornography, in violation of Title 18, United States Code, Section 2252(a)(2). I further submit that evidence relating to this crime, more particularly described in Attachment B, can be found at the Subject Premises, more particularly described in Attachment A.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

DEFINITIONS

5. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

a. "Cellular telephone" or "cell phone" means a hand held wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mails; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and

other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

b. "Child Pornography" is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

d. "Computer Server" or "Server," is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system (DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol

(IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

e. "Computer hardware" means all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer software" is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "Computer passwords, pass phrases and data security devices" consist of information or items designed to restrict access to or hide computer software,

documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

j. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. "Internet Service Providers" (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

l. "An Internet Protocol address" (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to it's destination. Most Internet service providers control a range of IP addresses. Some computers have static that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

m. "Hash Value" refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be

thought of as a "digital fingerprint" for data. If the data is changed, even very slightly (like the addition or deletion of a comma or a period), the hash value changes. Therefore, if a file such as a digital photo is a hash value match to a known file, it means that the digital photo is an exact copy of the known file.

n. "Media Access Control" (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

o. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

p. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs,

digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

q. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

r. "Visual depictions" include undeveloped film and videotape, and data stored on a computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

6. I have consulted in this matter with lay persons and law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. In particular, I have consulted with FBI SA Neil Lee, who has received specialized training as a forensic computer, cellular telephone, and other electronic storage device examiner. SA Lee has been a forensic computer examiner with the FBI since 2015. SA Lee has participated in the execution of numerous search warrants and search and seizure operations. SA Lee has informed me that to properly retrieve and analyze electronically stored computer data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is

necessary to conduct a forensic examination of the electronic storage devices. To achieve such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a form that becomes meaningful only upon forensic analysis.

7. Based on my knowledge, training, and experience, and after having consulted with SA Lee, I know that computer and other electronic device hardware, peripheral devices, software, documentation, and passwords may be important to a criminal investigation in three distinct and important respects.

a. The objects themselves may be instrumentalities used to commit the crime;

b. The objects may have been used to collect and store information about crimes (in the form of electronic data); and

c. The objects may be contraband or fruits of the crime.

8. I submit that if a computer or other electronic storage device is found on the premises, there is probable cause to believe those records will be stored in that electronic storage device, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person deletes a file on an electronic storage device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. It follows that deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone or tablet device) the device may also contain a record of deleted data in a swap or recovery file.

b. Wholly apart from user-generated files, electronic storage device and storage media in particular, computers internal hard drives contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users

typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

9. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how electronic storage devices were used, the purpose of their use, who used them, and when.

10. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record

additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was remotely accessed, thus inculpating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP

addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and timeline information described herein may either inculpate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage

device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

11. I know from my training and experience, as well as from information found in publicly available materials, that some electronic devices offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") which is read via an integrated biometric device in lieu of a numeric or alphanumeric passcode or password. This feature often referred to as a fingerprint scanner, a fingerprint reader, or for Apple devices, Touch ID.

12. If a user enables the fingerprint scanner on a given device, he or she can register multiple fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's fingerprint scanner, which can be found in different locations on the device depending on the manufacturer. In my training and experience, users of devices that offer

fingerprint scanners often enable it because it is considered a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

13. In some circumstances, a fingerprint cannot be used to unlock a device that has its fingerprint scanner enabled, and a passcode or password must be used instead. Thus, in the event law enforcement encounters a locked device, the opportunity to unlock the device via the fingerprint scanner exists only for a short time. The fingerprint scanner also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) too many unsuccessful attempts to unlock the device via the fingerprint scanner are made.

14. If fingerprint scanner enabled devices are found during a search of the premises, the passcode or password that would unlock such devices are presently unknown to law enforcement. Thus, it will likely be necessary to press the fingers of the user(s) of any device(s) found during the search of the premises to the device's fingerprint scanner in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the device(s) via fingerprint scanner with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

15. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via the fingerprint scanner, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Further, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the premises to press their finger(s) against the fingerprint scanner of the locked device(s) found during the search of the premises in order to attempt to identify the device's user(s) and unlock the device(s) via the fingerprint scanner.

16. Based upon my knowledge, training and experience, and after having consulted with SA Lee, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media, it is often necessary that some electronic storage device equipment, peripherals,

instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

17. In light of these concerns, I hereby request the Court's permission to seize the electronic storage devices, associated storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

18. I know that when an individual uses a computer to commit crimes involving child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe that an electronic storage device used to commit a crime of this type may contain: data that is evidence of how the electronic storage device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

PEER TO PEER PROGRAMS

19. Based on my training and experience, I know that a frequently employed method to share data over the Internet is Peer-to-Peer (P2P) file sharing. P2P file sharing

is a method of communication available to Internet users through the use of widely available software. The software is designed to allow users to trade digital files through the Internet. There are several different software applications that can be used to access these P2P networks and these applications operate in essentially the same manner.

20. To access the P2P networks, a user first obtains the P2P software, which can be downloaded free from the Internet. This software is used for sharing digital files. When the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available for download by any other user connected to the P2P network.

21. A user obtains files by conducting keyword searches of the P2P network. When a user initially logs onto the P2P network, a list of the files that the user is sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user looking to download files simply conducts a keyword search. The results supplied from that keyword search are displayed and the user then selects the file the user wants to download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer hosting the file. Once a file has been downloaded, it is stored in the area previously designated by the user and will remain there until moved or deleted. Most of the P2P software applications keep logs of each download event. Oftentimes, a forensic examiner, using these logs, can determine the IP address from which a particular file was obtained.

22. Most P2P software does not display the IP address of the person sharing the file to the user. Third party software is available to identify the IP address of the P2P computer sharing a particular file.

23. The BitTorrent network is a very popular and publicly available P2P file-sharing network. Most computers that are part of this network are referred to as "peers" or "clients." A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, including uTorrent, Vuze, and others. These are publicly available and typically free P2P client software programs that can be downloaded from the Internet. BitTorrent sets up its searches by keywords typically on torrent websites. The results of a keyword search are displayed to the user. The website does not contain the files being shared, only the file referred to as a "torrent." A torrent file defines the files being shared and contains file names, file sizes, file paths, the total number of pieces, the size of each piece, the SHA-1 hash value of each piece, and the torrent type (public or private). The torrent file does not contain the desired content; it simply defines what is available. A user may then select a torrent file from the search results for download.[1] For example, a person interested in obtaining child pornography images/videos could open the BitTorrent website on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The

[1] While multiple torrents can be downloaded simultaneously, this affidavit refers to a single file for clarity.

results of the search are returned to the user's computer and displayed on the torrent site. The user selects a torrent from the results displayed the file the user wants to download. Once the torrent file is downloaded, the user's previously installed BitTorrent client program utilizes the torrent file to obtain the desired content on the network. The file is downloaded directly from the computer or computers sharing the file. The users can receive pieces of the selected file from numerous sources at once. Once received, the pieces are then reassembled into the entire selected file. The downloaded file is stored in a folder previously designated by the user and/or the client program on the user's computer or designated external storage media or location on the user's computer. The downloaded file will remain until moved or deleted.

24. An "info hash" is used to identify a unique torrent. For example, when a client establishes communication with a peer, it identifies the torrent that it is interested in by providing the info hash. The info hash assures that all the values in the info section of the torrent that is sought are identical to the values of the info section in the target's torrent.

DETAILS OF THE INVESTIGATION

25. On November 21, 2019, between 12:04 AM and 12:20 AM, an FBI Special Agent acting in an undercover capacity (UC-1), was connected to the Internet and using BitTorrent. UC-1 directly connected to a device at IP address 174.97.134.56 and successfully downloaded 2 files that the device at IP address 174.97.134.56 was making available. IP Address 174.97.134.56 was the only IP address that shared the contents for

each file downloaded, and as such, each file was downloaded directly from this IP address.

26. I reviewed the one of the downloaded files and saw it included the following:

a. Video file: **(**Pthc)-8Yo Boy Fucks 6Yo Girl, She Cries For Mom (English).avi which depicts a juvenile male wearing a striped-shirt and dark colored pants which are pulled down exposing his buttocks. The juvenile is having intercourse with a juvenile female who is bent over at the waist positioned rear facing over a toilet. The female is wearing a light-colored garment which is pulled up to expose her buttocks towards the male.

27. On February 20, 2020, between 12:48 AM and 01:10 AM, an FBI Special Agent acting in an undercover capacity (UC-1), was connected to the Internet and using BitTorrent. UC-1 directly connected to a device at IP address 174.97.134.56 and successfully downloaded multiple partial files that the device at IP address 174.97.134.56 was making available. IP Address 174.97.134.56 was the only IP address that shared the contents for each file portion downloaded, and as such, each file portion was downloaded directly from this IP Address.

28. I reviewed multiple partial downloaded files and saw they included some the following:

a. Video file: 10-12Yo Boy's Masturbation.mpg depicts two prepubescent fully nude Asian boys sitting next to one another masturbating each other.

b. Video file: bibcam - 12yo and 14yo boys blow and fuck for a long time. HiRes. Gay, Pedo, Preteen, PJK..mpg depicts two prepubescent fully nude males having oral sex.

c. Video file: Gay – Man Fucks 12Yo Boy.mpg depicts a pre-pubescent female lying naked on her back with nude a young male positioned on top of her. The male is penetrating her vagina with his fingers while the female is giving oral sex to the male.

29. In December 2019 and March 2020, FBI Operational Support Technician Andrew Boese issued an administrative subpoena to Charter Communications on two separate instances. SA George K Mason reviewed both responses and determined the IP address 174.97.134.56 was assigned from 10/13/2017 to 3/11/2020 to:

Name: Donald Griego

Service Address: 2611 S. Shore Drive

City/State/Zip: Milwaukee, Wisconsin, 53207

Telephone: 414-744-3588

Email: mrdgriego@gmail.com

30. In August 2020, FBI Operational Support Technician Andrew Boese issued an administrative subpoena to Charter Communications on address 2611 S. Shore Drive, Milwaukee, Wisconsin, 53207. SA George K Mason reviewed the response and determined an IP address of 72.128.65.122 assigned from 04/03/2020 to 08/10/2020:

Name: Mr Donald Griego

Account: 8334902

Service Address: 2611 S. Shore Dr

City/State/Zip: Milwaukee, Wisconsin, 53207

Telephone: 414-744-3588

Email: mrdgriego@gmail.com

31. On March 21, 2020, between 07:00 AM and 07:10AM, a sworn Law Enforcement Officer acting in an undercover capacity (UC-2), was connected to the Internet and using BitTorrent. UC-2 directly connected to a device at IP address 72.128.65.122 and successfully downloaded files that the device at IP address 72.128.65.122 was making available. IP Address 72.128.65.122 was the only IP address that shared the contents for each file portion downloaded, and as such, each file portion was downloaded directly from this IP Address.

32. I reviewed multiple downloaded files and saw they included some the following:

a. Video file: 000283.avi depicts a nude female approximately 10 to 13 years of age and an adult male. The female was kneeling with her breasts exposed and was performing oral sex on a standing adult male.

b. Video file: 000284.avi depicts a prepubescent nude female approximately 8 to 10 years of age first standing with her hands behind her head exposing her breasts and vagina. As the video continues it shows the female lying on

her back with her breasts and vagina exposed. Lastly, the video depicts a penis penetrating the females vagina in a back and forward motion.

33. Based upon the above information and my training and experience, I believe the above videos are child pornography as the statute and this search warrant affidavit define it.

34. On July 13, 2020, the FBI conducted physical surveillance at 2611 S. Shore Drive, Milwaukee, Wisconsin. During that time the following observations took place:

a. A 2013 Honda Civic, bearing Wisconsin tag 918-NVL registered to Cielo Alberto Griego, 2611 S. Shore Drive, Milwaukee, Wisconsin.

b. Cielo Griego was observed exiting 2611 S. Shore Drive, Milwaukee, Wisconsin and removed the tag 918-NVL from the 2013 Honda Civic and replaced it with temporary tag B5976DE.

c. Utilizing the 2013 Honda Civic, Cielo Griego was observed travelling to Meijer, 5800 West Layton Avenue, Greenfield Wisconsin.

d. With the same vehicle, Griego departed Meijer and drove to Pick 'n Save, 250 West Holt Avenue, Milwaukee, Wisconsin.

e. Cielo Griego returned to 2611 S. Shore Drive, Milwaukee, Wisconsin and entered into the residence.

35. On July 28th 2020, the FBI conducted physical surveillance at 2611 S. Shore Drive, Milwaukee, Wisconsin. During that time the following observations took place:

a. A 2013 Honda Civic, bearing Wisconsin temporary tag B5976DE, registered to Cielo Alberto Griego, 2611 S. Shore Drive, Milwaukee, Wisconsin.

b. A grey Subaru Crosstrek, bearing Wisconsin tag 519-ZMR, registered to Santa Griego, 2611 S. Shore Drive, Milwaukee, Wisconsin.

c. The following subjects were observed:

i. Cielo Griego, son of Donald Griego

ii. Donald Griego, father of Cielo Griego

iii. Santa Arriaga Griego, mother of Cielo Griego and spouse of Donald Griego

36. On October 19th, 2020 the FBI conducted physical surveillance at 2611 S Shore Drive, Milwaukee, Wisconsin. During that time the following observation took place:

a. A gray 2013 Honda Civic, bearing Wisconsin tag AJX7357, registered to Cielo Alberto Griego, 2611 S Shore Drive, Milwaukee, Wisconsin, parked outside on the east side of the residence 2611 S Shore Drive, Milwaukee, Wisconsin, on S. Shore Drive.

BACKGROUND ON ELECTRONIC STORAGE DEVICES AND CHILD PORNOGRAPHY

37. Computers, cellular telephones, and other electronic storage devices (collectively electronic storage devices) have dramatically changed the way in which individuals interested in child pornography interact with each other. Electronic storage devices basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

38. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a device by simply connecting the camera to the electronic storage device. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video recorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the video recorder to a computer. Many electronic storage devices (e.g., computers, cellular telephones, and tablets), have cameras built into the device which allows users to create and store still and video images on the device. Moreover, if the device has internet connectivity, users can distribute still and video images from the device.

39. Internet-enabled electronic storage devices can connect to other internet-enabled devices the world over. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to an internet-enabled electronic storage

device. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, electronic storage devices are the preferred method of distribution and receipt of child pornographic materials.

40. Electronic storage devices are an ideal repository for child pornography. The amount of information that an electronic storage device can hold has grown exponentially over the last decade. Electronic storage devices can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on a computer or other electronic storage device. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Many electronic storage devices can easily be concealed and carried on an individual's person.

41. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

42. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote

computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any internet-enabled electronic storage device. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's electronic storage device in most cases.

43. As is the case with most digital technology, communications by way of electronic storage device can be saved or stored on the device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, an electronic storage device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

44. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file

does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

CONCLUSION

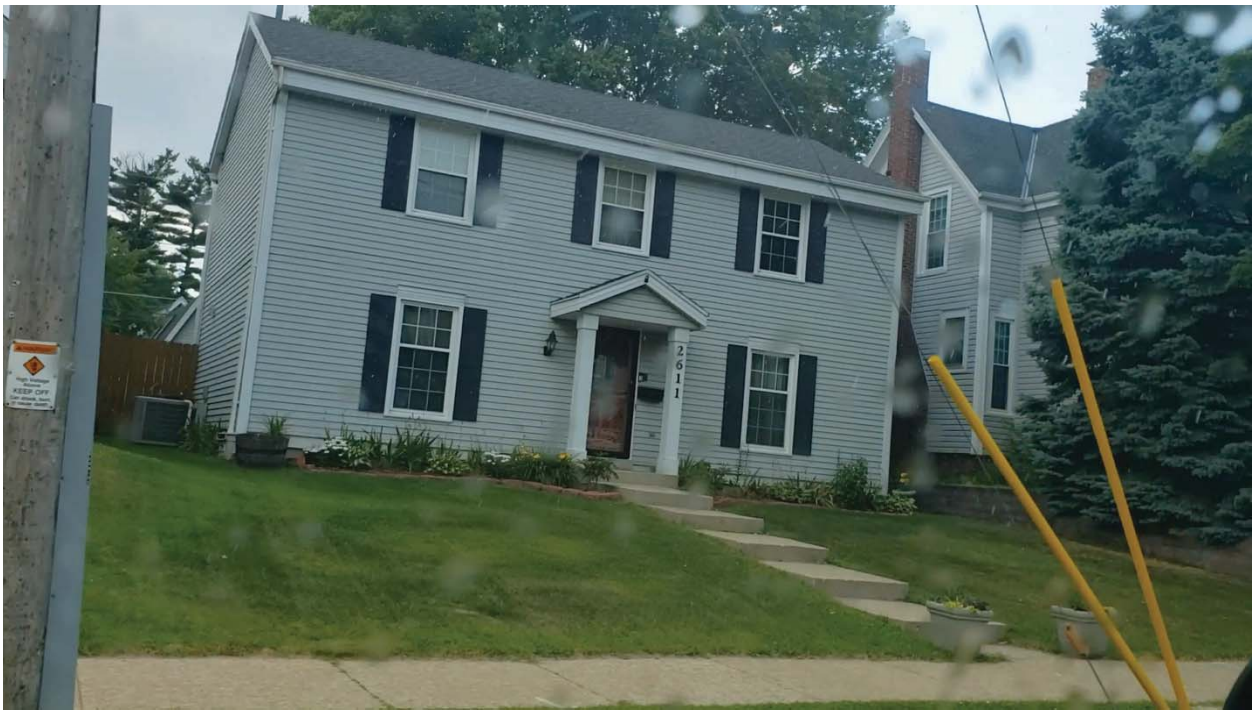
45. I submit that this affidavit supports probable cause for a warrant to search the premises described in Attachment A and seize the items described in Attachment B.

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at 2611 S. Shore Drive, Milwaukee, Wisconsin, including the residential building, any outbuildings, and any appurtenances thereto. 2611 S. Shore Drive, Milwaukee, Wisconsin is further described as a two-story, single family house, with light grey colored siding, white windows with dark shutters, and dark-colored shingles. On the front of the house is a dark colored storm-door and what appears to be a wooden door behind it with a large oval shaped glass insert. To the right of the door is a black mailbox. On both sides of the door are two porch lights. Affixed to the supporting column of the entry overhang are the numerals "2611" in large black numbers, on a white background. There are entry stairs leading to the front door from the public sidewalk alongside Shore Drive. The residence driveway and garage is on the rear side of the house off the alleyway, and leads to a single garage door in the rear of the house. The garage is not attached to the house. It has light colored siding with a white garage door and a white entry door

Photos taken of the residence on July 7, 2020 are as follows:


2611

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Cell phones, computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of

minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of any device by use of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all notes, documents, records, or correspondence, in any format or

medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment.

13. Any and all visual depictions of minors.

14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. For any electronic storage device, computer hard drive, electronic device, or other physical object upon which electronic information can be recorded (hereinafter, "electronic storage device") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant

messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;

e. evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage device;

h. evidence of the times the electronic storage device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;

j. documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;

k. contextual information necessary to understand the evidence described in this attachment.

17. Records and things evidencing the use of the Internet Protocol addresses to communicate with the internet, including:

a. routers, modems, and network equipment used to connect electronic storage devices to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the premises to the Touch ID sensor of Apple brand device(s) or scan for facial recognition, such as an iPhone or iPad, found at the premises for the purpose of attempting to unlock the device via Touch ID or Face ID in order to search the contents as authorized by this warrant. If Face ID is required, the subject(s) will remain still and look, with eyes open, at the camera for any devices seized in connection if this warrant for the

purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.